D5.2 Trials Setup

Work Package: WP5

Lead partner: Comune di Bologna (BOL)

Author(s): Giovanni Farneti (BOL), Rosella Mancilla, Barbara Pirillo (ENG), Nadezhda Ilina, Amedeo D’Arcangelo (KSP-IT), Luigi Sgaglione (CINI), Felipe Apolinario (INOV), Cornelia Gerdenitsch (AIT), Iker Muñiz (S21Sec), Almerindo Graziano (GNSIL), Alexander Krock (NIT).

Due date: 31st October 2018

Version number: 2.0 Status: Final version - revised

Grant Agreement N°: 740712

Project Acronym: COMPACT

Project Title: COMPetitive Methods to protect local Public Administration from Cyber security Threats

Call identifier: H2020-DS-2016-2017

Instrument: IA

Thematic Priority: Secure societies – Protecting freedom and security of Europe and its citizens

Start date of the project: May 1st, 2017

Duration: 30 months

<table>
<thead>
<tr>
<th>Dissemination Level</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PU: Public</td>
<td>✓</td>
</tr>
<tr>
<td>PP: Restricted to other programme participants (including the Commission)</td>
<td></td>
</tr>
<tr>
<td>RE: Restricted to a group specified by the consortium (including the Commission)</td>
<td></td>
</tr>
<tr>
<td>CO: Confidential, only for members of the consortium (including the Commission)</td>
<td></td>
</tr>
</tbody>
</table>

Project co-funded by the European Commission under the Horizon 2020 Programme.
## Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Who</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>19/10/2018</td>
<td>BOL</td>
<td>First draft with TOC</td>
</tr>
<tr>
<td>0.2</td>
<td>26/10/2018</td>
<td>BOL, ENG, KSP-IT</td>
<td>Second draft</td>
</tr>
<tr>
<td>0.3</td>
<td>30/10/2018</td>
<td>BOL, CINI, INOV</td>
<td>Third draft</td>
</tr>
<tr>
<td>0.4</td>
<td>31/10/2018</td>
<td>BOL, ENG</td>
<td>Final draft with checklist</td>
</tr>
<tr>
<td>1.0</td>
<td>6/11/2018</td>
<td>BOL, AIT, S21SEC, GNSIL</td>
<td>Final edit</td>
</tr>
<tr>
<td>1.1</td>
<td>8/11/2018</td>
<td>BOL, ENG</td>
<td>Final edit with final amendments</td>
</tr>
<tr>
<td>2.0</td>
<td>27/05/2019</td>
<td>BOL, INOV, BIT</td>
<td>Revised version (after 2\textsuperscript{nd} project review)</td>
</tr>
</tbody>
</table>

## Quality Control

<table>
<thead>
<tr>
<th>Role</th>
<th>Date</th>
<th>Who</th>
<th>Approved/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Reviewer</td>
<td>6/12/2018</td>
<td>GNSIL</td>
<td>Approved with comments</td>
</tr>
<tr>
<td>Internal Reviewer</td>
<td>6/12/2018</td>
<td>KSP-IT</td>
<td>Approved with comments</td>
</tr>
</tbody>
</table>
Disclaimer:

This document has been produced in the context of the COMPACT Project. The COMPACT project is part of the European Community’s Horizon 2020 Program for research and development and is as such funded by the European Commission. All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability with respect to this document, which is merely representing the authors’ view.
Table of Contents

Executive Summary ........................................................................................................... 8
1. General procedure ...........................................................................................................8
2. Trial Setup Plan .............................................................................................................8
   2.1. COMPACT Communication Bus ............................................................................ 10
   2.2. COMPACT Dashboard .........................................................................................10
   2.3. LPA Training ..........................................................................................................11
3. Trial Tools Setup ..........................................................................................................12
   3.1. BIT – Municipality of Bremerhaven ....................................................................12
       3.1.1. RATING ........................................................................................................... 12
       3.1.2. TO4SEE ......................................................................................................... 13
       3.1.3. HFP ................................................................................................................ 14
       3.1.4. Openness.edu ................................................................................................. 15
       3.1.5. KIPS ............................................................................................................... 16
       3.1.6. SOC ............................................................................................................... 17
       3.1.7. SENTINEL ...................................................................................................... 18
       3.1.8. CyberConnector ............................................................................................... 19
       3.1.9. Communication bus ....................................................................................... 20
       3.1.10. Dashboard ...................................................................................................... 20
   3.2. BOL – Municipality of Bologna ..........................................................................21
       3.2.1. RATING ........................................................................................................... 21
       3.2.2. TO4SEE ......................................................................................................... 21
       3.2.3. Openness.edu ................................................................................................. 22
       3.2.4. CSMG ............................................................................................................ 22
       3.2.5. CyberConnector ............................................................................................... 23
       3.2.6. Communication Bus ....................................................................................... 23
       3.2.7. Dashboard ...................................................................................................... 23
   3.3. CDA – Municipality of Afragola ...........................................................................24
       3.3.1. RATING ........................................................................................................... 24
       3.3.2. TO4SEE ......................................................................................................... 24
       3.3.3. KIPS ............................................................................................................... 24
       3.3.4. SOLE ............................................................................................................. 25
       3.3.5. SOC ............................................................................................................... 27
       3.3.6. Openintel ........................................................................................................ 30
       3.3.7. CyberConnector ............................................................................................... 31
       3.3.8. Communication bus ....................................................................................... 31
       3.3.9. Dashboard ...................................................................................................... 31
   3.4. CMA – Municipality of Amadora .........................................................................32
       3.4.1. RATING ........................................................................................................... 32
       3.4.2. TO4SEE ......................................................................................................... 32
       3.4.3. SOC ............................................................................................................... 32
       3.4.4. BP-IDS ......................................................................................................... 32
       3.4.5. MISP ............................................................................................................. 40
       3.4.6. Communication bus ....................................................................................... 41
3.4.7. Dashboard ................................................................. 41
3.5. DSS – Municipality of San Sebastian ............................................. 42
  3.5.1. RATING ............................................................. 42
  3.5.2. TO4SEE ........................................................... 42
  3.5.3. HFP ............................................................... 43
  3.5.4. KIPS ............................................................... 45
  3.5.5. SOLE ............................................................ 46
  3.5.6. SOC ............................................................... 47
  3.5.7. SENTINEL ......................................................... 47
  3.5.8. Communication bus ....................................................... 47
  3.5.9. Dashboard ........................................................... 47
4. Checklist for research involving human participants ............................... 48
List of Figures

Figure 1 - RATING’s Self Assessment Questionnaire .......................................................... 12
Figure 2 - Example of TO4SEE’s content localization for Germany .................................. 13
Figure 3 - Second example of TO4SEE’s content localization for Germany ...................... 13
Figure 4 - Third example of TO4SEE’s content localization for Germany ......................... 14
Figure 5 - SOC Dashboard: sources view ......................................................................... 18
Figure 6 - SOC Dashboard: SENTINEL View ..................................................................... 18
Figure 7 - Sentinel dashboard ............................................................................................ 18
Figure 8 - COMPACT Information Hub multi-language easy access ................................... 19
Figure 9 - Example of TO4SEE’s content localization for Italy ........................................ 21
Figure 10 - Second example of TO4SEE’s content localization for Italy .......................... 22
Figure 11 - MISP-related training available on SOLE for the COMPACT users ............. 25
Figure 12 - VPN instructional videos .................................................................................. 26
Figure 13 - SOC dashboard .............................................................................................. 30
Figure 14 - Diagram representing the BP-IDS installation made on the IT infrastructure of the municipality of Amadora. Connection between systems coloured in black are interactions that currently occur in the IT infrastructure. While the blue connections, are the additional connections required for BP-IDS to monitor database activity ....................................................... 33
Figure 15 - Configuration required for tracer DLL activation using the ODBC Data Source Administrator .............................................................................................................. 35
Figure 16 - CMA network topology, describing all the information required to establish communication between all BP-IDS components and to determine where to collect the traces. The information provided includes, the IP address and location in the network of all BP-I ............................................................................................................................................... 36
Figure 17 - GANTT diagram that schedules all the action plan tasks proposed in this document. The tasks are distributed across the vertical axis, while the horizontal axis shows the evolution of time in months from the first release of the COMPACT platform to the last COMPACT trial ................................................................. 38
Figure 18 - MISP sample deployment .................................................................................. 40
Figure 19 - Example of TO4SEE’s content localization for Portugal ................................. 42
Figure 20 - Second example of TO4SEE’s content localization for Portugal .................... 43
Figure 21 - Third example of TO4SEE’s content localization for Portugal ....................... 43

List of Tables

Table 1 - COMPACT Trials ................................................................................................. 9
Table 2 - COMPACT KIPS and CSMG Training ............................................................... 11
Table 3 - Business process information, describing for each monitored process all the information required to identify the activities and resources linked to the monitored process and to perform incident detection. The figure on the left shows the information related with the process ‘Emission of certification’, while the figure on the right is related with process ‘Assiduity Management’ ......................................................................................................................... 37
## Definitions and acronyms

<table>
<thead>
<tr>
<th>CC</th>
<th>CyberConnector</th>
</tr>
</thead>
<tbody>
<tr>
<td>CyberConnector</td>
<td>An internal knowledge collaboration site and social network that is used to share all the information among partners. Referred to also as CC.</td>
</tr>
<tr>
<td>DoA</td>
<td>Description of Action</td>
</tr>
<tr>
<td>MST</td>
<td>Management and Support Team</td>
</tr>
<tr>
<td>PC</td>
<td>Project Coordinator</td>
</tr>
<tr>
<td>SC</td>
<td>Scientific Coordinator</td>
</tr>
<tr>
<td>BP-IDS</td>
<td>Business Process based Intrusion Detection System</td>
</tr>
<tr>
<td>CC</td>
<td>CyberConnector</td>
</tr>
<tr>
<td>LPA</td>
<td>Local Public Administration</td>
</tr>
<tr>
<td>BIT</td>
<td>BIT - WIRTSCHAFTSBETRIEB DER STADT BREMERHAVEN (DE)</td>
</tr>
<tr>
<td>BOL</td>
<td>Comune di Bologna (IT)</td>
</tr>
<tr>
<td>CDA</td>
<td>Comune di Afragola (IT)</td>
</tr>
<tr>
<td>CMA</td>
<td>Municipio de Amadora (PT)</td>
</tr>
<tr>
<td>DSS</td>
<td>Donostia San Sebastian (ES)</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
</tbody>
</table>
Executive Summary

This document aims at describing the activities carried out to set up trials in every LPA involved in the COMPACT project, in terms of configuration, installation, localization and customization of the COMPACT tools. The outcome is to demonstrate the actual process of trials being carried out in every City, performed by different tools providers. Thus, the general structure of this demonstrator is LPA based.

1. General procedure

The approach to the trial validation of the COMPACT project aims at experimenting all the tools of the COMPACT services in the 5 project LPAs (see Table 5 of Deliverable 5.1 “Validation and Demonstration scenarios – revised version”). Every LPA will test at least 5 tools on 2 scenarios in operative environment, for a total of 268 participants and 32 versions of tools to be tested (see Table 6 of Deliverable 5.1 “Validation and Demonstration scenarios - revised version”).

2. Trial Setup Plan

A full picture of all the tools to be tested in every LPA is shown on Table 1, with relevant scenarios, number of participants, language localizations and type of installations.
<table>
<thead>
<tr>
<th>LPA</th>
<th>Scenarios</th>
<th>Part.</th>
<th>Tools</th>
<th>Language</th>
<th>Type of installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIT</td>
<td>Channelling the information</td>
<td>20</td>
<td>RATING TO4SEE HFP</td>
<td>English</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Openness.edu</td>
<td>German</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>KIPS</td>
<td>German</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SOC</td>
<td>German</td>
<td>Cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SENTINEL</td>
<td>English</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CyberConnector</td>
<td>English</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td>Improvement of network monitoring through the use of additional tools</td>
<td>8</td>
<td>RATING TO4SEE HFP Openness.edu KIPS SOC SENTINEL CyberConnector</td>
<td>English</td>
<td>Cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>German</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>German</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>English</td>
<td>SaaS</td>
</tr>
<tr>
<td>BOL</td>
<td>Overcoming psychological barriers</td>
<td>40</td>
<td>RATING TO4SEE Openness.edu</td>
<td>English</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td>Securing ubiquitous Smart Working: identification of residual risks</td>
<td>100</td>
<td>CSMG CyberConnector</td>
<td>Italian</td>
<td>Cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Italian</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Italian</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Italian</td>
<td>Cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>English</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>English</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td>Supporting interaction between expert and non-expert employees</td>
<td>9</td>
<td>RATING TO4SEE KIPS SOLE SOLE Openintel CyberConnector</td>
<td>English</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td>Protecting against bad habits in the workplace</td>
<td>9</td>
<td></td>
<td>Italian</td>
<td>Cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Italian</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Italian</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>English</td>
<td>SaaS</td>
</tr>
<tr>
<td>CDA</td>
<td>Supporting standards-based ISMS implementation</td>
<td>15</td>
<td>RATING TO4SEE SOC BP-IDS MISP</td>
<td>English</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td>Monitoring GDPR compliance</td>
<td>5</td>
<td></td>
<td>Portuguese</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>English</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>English</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>English</td>
<td>SaaS</td>
</tr>
<tr>
<td>DSS</td>
<td>Achieving compliance in risk management</td>
<td>32</td>
<td>RATING TO4SEE HFP KIPS SOLE SOLE SENTINEL</td>
<td>English</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td>Continuous and adaptive improvement of cybersecurity awareness</td>
<td>30</td>
<td></td>
<td>Spanish+Basque</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Spanish+Basque</td>
<td>SaaS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Spanish+Basque</td>
<td>Cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Spanish+Basque</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>English</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>English</td>
<td>Local</td>
</tr>
</tbody>
</table>

Table 1 - COMPACT Trials
2.1. COMPACT Communication Bus

The COMPACT Communication Bus is in charge of delivering the data and messages between all COMPACT components and between data sources and SIEM components. It is a communication channel with high performance in terms of throughput, scalability, and reliability and with a very low overhead for the clients that want to use it. The selected paradigm used to implement the event bus is the publish/subscribe one, that is a messaging pattern where senders of messages, called publishers, do not send the messages directly to specific receivers, but instead publish them into specific "locations" called topics where the interested parties (called subscribers) can be subscribed in order to receive the published messages. This paradigm is one of the key element of the loosely coupled architecture that characterizes the COMPACT platform. From a technology point of view, the communication bus has implemented using Apache KAFKA.

Considering that some of the tools provided by COMPACT need to be installed on LPA premises or at least to have access to LPA local data, and some other tools are instead available online (web services), the Communication bus will serve also as bridge between the LPA local infrastructure and the COMPACT web services. When possible, the Communication bus will be installed in the LPA infrastructure and connected to both the LPA local network and with the Virtual Private Network (VPN) provided by COMPACT in order to allow a secure communication between remote and local COMPACT tools. Furthermore, to allow a separation between LPAs data, each LPA will have a dedicated COMPACT Communication bus.

2.2. COMPACT Dashboard

The COMPACT Dashboard helps visualizing all the data and messages generated by COMPACT tools by a set of graphs. As the information generated by COMPACT is drastically sensitive for the LPA security, COMPACT Dashboard implements user access control to preserve the confidentiality of the information. The COMPACT Dashboard includes information regarding risk assessment, educational services, monitoring services and communications.

COMPACT Dashboard is fully scalable, in other words, if new tools are added, the graphs will show automatically based on the COMPACT Communication Bus. In addition, COMPACT, by default, is fully independent among LPAs as it only gathers information from COMPACT Communication Bus.

COMPACT Dashboard gathers information from the COMPACT Communication Bus (refer to chapter 2.1 for more details). Given the implementation above, COMPACT Dashboard will act as a subscriber of the COMPACT Communication Bus. As COMPACT Dashboard uniquely
depends on the COMPACT Communication Bus, it will be installed locally in each LPA if possible.

2.3. LPA Training

In order to perform training session in every LPA involved in the testing of CSMG and KIPS tools, a set of training sessions for local trainers has been scheduled.

For CSMG a 2 days live training will occur in November 2018, involving 4 potential trainers from the Municipality of Bologna.

For KIPS 2 on-line sessions of 3 hours are foreseen by December 2018 and will involve 2 representative potential trainers from each Municipalities of Afragola, Amadora, Bremerhaven and San Sebastian.

The complete list of potential trainers is shown on Table 2.

<table>
<thead>
<tr>
<th>Tool</th>
<th>LPA</th>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSMG</td>
<td>BOL</td>
<td>Giovanni Farneti</td>
<td><a href="mailto:giovanni.farneti@comune.bologna.it">giovanni.farneti@comune.bologna.it</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rosanna Vallarelli</td>
<td><a href="mailto:rosanna.vallarelli@comune.bologna.it">rosanna.vallarelli@comune.bologna.it</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Christian Baraldi</td>
<td><a href="mailto:christian.baraldi@comune.bologna.it">christian.baraldi@comune.bologna.it</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matteo Melotti</td>
<td><a href="mailto:matteo.melotti@comune.bologna.it">matteo.melotti@comune.bologna.it</a></td>
</tr>
<tr>
<td>KIPS</td>
<td>BIT</td>
<td>Alexander Krock</td>
<td><a href="mailto:Alexander.Krock@bit.bremerhaven.de">Alexander.Krock@bit.bremerhaven.de</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Benjamin Eden</td>
<td><a href="mailto:Benjamin.Eden@bit.bremerhaven.de">Benjamin.Eden@bit.bremerhaven.de</a></td>
</tr>
<tr>
<td></td>
<td>CDA</td>
<td>Andrea Rescigno</td>
<td><a href="mailto:andrea.rescigno82@gmail.com">andrea.rescigno82@gmail.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pasquale Vollaro</td>
<td><a href="mailto:vollaro.pas@gmail.com">vollaro.pas@gmail.com</a></td>
</tr>
<tr>
<td></td>
<td>CMA</td>
<td>Francisco José de Sousa Cruz</td>
<td><a href="mailto:francisco.cruz@cm-amadora.pt">francisco.cruz@cm-amadora.pt</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ricardo Jorge Faria Simões</td>
<td><a href="mailto:ricardo.simoes@cm-amadora.pt">ricardo.simoes@cm-amadora.pt</a></td>
</tr>
<tr>
<td></td>
<td>DSS</td>
<td>Paco Abal</td>
<td><a href="mailto:paco_abal@donostia.eus">paco_abal@donostia.eus</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Asier Alkorta</td>
<td><a href="mailto:asier_alkorta@donostia.eus">asier_alkorta@donostia.eus</a></td>
</tr>
</tbody>
</table>

Table 2 - COMPACT KIPS and CSMG Training
3. Trial Tools Setup

3.1. BIT – Municipality of Bremerhaven

3.1.1. RATING

RATING is the tool that generates a risk profile of the LPA through the completion of a Risk assessment. It is developed to be used by a representative of the LPA who has the knowledge and enough security experience to fulfil the security risk assessment. For this reason, the tool has no need to be translated or localized (see D5.1).

![Figure 1 - RATING's Self Assessment Questionnaire](image)

RATING is a SaaS, available to all LPAs in the consortium and is not customized for single LPA. It is hosted by ENG’s servers and for the field trials, it will be available under COMPACT VPN.

The RATING’s adaptation to COMPACT requirements has required the definition of an adapter to convert RATING’s output to other COMPACT components’ needs and to forward the risk profile refinement request to RATING (for details on RATING ‘s adaptation see D4.2).

The adapter has also the function to sort RATING’s outputs to the correct instances of the COMPACT Communication Bus due to the SaaS type of RATING installation and the configuration of field trials: the adapter could be configured to interact with different instances of Communication Buses, details are available in D4.2.

The tool will be available at the end of November 2018 for the start of the first trial phase.

A second version of the tool, revised and tuned by feedback collected at the end of the first phase will be released at the end of April 2019.
3.1.2. TO4SEE

TO4SEE is the tool measuring the improvements of people on the knowledge of phishing email.

As described into D4.2 the tool will be included in Openess.edu’s content: it is configured as an individual assessment to be performed before and after training sessions.

This tool will be used in all of the field trials by LPA’s employees, therefore TO4SEE will be available to generic users translated and localized for each LPA in the consortium.

The first version will be available at the end of November 2018. If necessary, the tool will be re-tuned after the end first trial phase (May 2019).

For the field trials in Bremerhaven Municipality (BIT), TO4SEE’s content has been translated into German and some of them localized to German context.

---

**Figure 2 - Example of TO4SEE's content localization for Germany**

**Figure 3 - Second example of TO4SEE's content localization for Germany**
3.1.3. HFP

The Human Factor Profile is a survey instrument which can be used to investigate human predictors of security-related behaviour. In particular, HFP depicts six human factors that have been proven to influence security-related behaviour. Results should guide the management of an organisation to choose suitable awareness methods. In addition, it provides the management with data that describe work-related, organizational, and other individual variables that are relevant in this context.

- **Configuration:** Configuration: please specify if the tool will be customized for that LPA and how; The tool will not be customized for the specific LPA, as the human factors that are analysed are generalizable across organizations.
- **Installation:** There is no installation or training needed. To guide users, we provide an instruction about how to proceed with the HFP.
- **While the tool is made available and ready in November, before the trials, the process for analysis is done manually. The link to the HFP tool in English is available from [https://surveys.tech-experience.at/index.php/731494?lang=en](https://surveys.tech-experience.at/index.php/731494?lang=en). A detailed description can be found in D4.2.

Instruction for using HFP presented to the LPAs to guide them in using HFP.

General Information: The Human Factor Profiling method is a survey instrument that should help you to understand why people within your organisation act security-aware. This information should guide you in choosing the most suitable awareness method for your employees. The link is meant to be spread to the employees in your organisation.
Please be aware that due to anonymity reasons we will only analyze the data and provide you with results when more than three employees filled out the survey.

Procedure: Before using this survey please be aware of informing all relevant stakeholders within your organization including the workers’ council or the data protection officer. This can increase the acceptance of this survey significantly. We also recommend informing employees about the results of the survey in a workshop setting.

Return Rates: The higher the return rates the higher is the validity of the results for your specific organisation. We recommend sending two reminders; one after one week and one two days before the survey will be closed.

For the creation of the survey link and for our analyses we need some information from you: Name of your organisation in this field (also a fictional name is possible): _________
Number of employees that will get the link to the survey: ______
Here is the Human Factor Profiling survey link: ______________

Please spread this link in your organisation for example via e-mail or intranet. Thereby, you can use the following text and adapt it according to your personal preferences:

“Maintaining security in an organisation is increasingly important. We at <organisation name> are interested in investigating how to provide you with suitable training to increase security-related behaviour and thus make our organisation resilient against a potential cyber-attack. This survey should help us to understand why people within our organisation act security-aware and how to support them in acting more security-aware. The information collected within the survey guides us to choose the most suitable awareness methods we can use in training. So, the more survey data we get the more tailored our training can be.

Here is the link to the survey which will be sent to all employees: <insert survey link in here>. The survey is open for two weeks.

Please be aware that this data will be analysed in an aggregated way with at least three data sets. So, there is no possibility to draw conclusions to the individual employee. If you have any questions please contact me.”

<table>
<thead>
<tr>
<th>3.1.4. Openness.edu</th>
</tr>
</thead>
</table>

For COMPACT field trials Openness.edu is a Cloud-based platform created to provide awareness content on security in general. It is based on role separation of users. Four user groups have been identified to follow COMPACT requirements: CERT expert, that creates new courses and define the “training set”, LPA CyberSecurity expert that defines the “training plan” for each kind of employee, the LPA CyberSecurity Manager, that verifies if the employees follow the plan and the LPA Employee that play courses in his training plan.

Openness.edu in COMPACT version interacts with RATING tool providing the anonymized information about the “Individual Assessment” of each employee.

Openness.edu does not need to be configured providing service to different LPA. Everything is done when the users will be uploaded.
Openness.edu provides a well-stocked list of localizations: for the field trial in the Municipality of Bremerhaven Openness.edu will be used in German with German content.

The component is a web application running in the cloud deployed on ENG’s servers. During the field trials, Openness.edu will be available inside the COMPACT VPN.

The user profiling is defined internally for the first phase trial. In the second phase will be introduced the COMPACT common tool for user management.

The basic tool is running by end of October 2018 and it will be settled up and configured during November 2018.

3.1.5. KIPS

Custom-built software simulates the impact cyber-attacks and associated management decisions can have on business performance and revenue. Gameplay develops an understanding of cybersecurity measures. KIPS establishes a better security understanding among senior managers and decision makers, increases awareness of the risks and security problems of running modern computerized systems.

Specialized KIPS scenario is being developed for LPAs under COMPACT project, viewing the threats especially important for understanding by LPA management.

The scenario will be localized into German.

There are following scenario components to be localised:

- Scenario components
  - Game Board
  - Action Cards
  - Messages
  - Game Rules PPT
  - Scenario constants
  - Interface Constants
  - Certificates default texts
  - Feedback Form

The localization is to be performed by partner LPAs after they are provided with all the source files (e.g. Adobe Illustrator files for graphics, PHP files for messages, XLS files for Constants and PPT file for Game Rules).

KIPS is a SaaS application, accessible from Kaspersky Lab server. In order to run KIPS, a specialised training for trainers is required (2 remote sessions on Webex, 3 hours each).
Timeframe:

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alfa-version of KIPS LPA Scenario</td>
<td>Nov 2018</td>
</tr>
<tr>
<td>TTT for trainers from partner LPAs</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>Trials for LPAs</td>
<td>Dec 2018 – Jan 2019</td>
</tr>
<tr>
<td>Feedback processing and implementation of changes</td>
<td>Jan-March 2019</td>
</tr>
<tr>
<td>Integration (data level) with Compact platform</td>
<td>Feb-Apr 2019</td>
</tr>
</tbody>
</table>

Link: KIPS is a session-based on-site or online game that is not available out of the session time. More information: [https://www.kaspersky.com/enterprise-security/security-awareness](https://www.kaspersky.com/enterprise-security/security-awareness)

3.1.6. SOC

Inside the BIT LPA, the SOC component will be used only as presentation layer of the other security monitoring tools involved in the BIT scenario. In order to achieve that a light version of the SOC will be installed (the possibility of full SOC usage will be evaluated during the first trial phase and made available - if required by the LPA - during the second phase). This version includes all software needed to allow the data acquisition of event from the security monitoring tools, the data storage and the data presentation via the SOC dashboard. This light version will be installed in the same machine of the COMPACT Communication bus. The SOC dashboard provides a unified view of all data sources available for the BIT scenario and also a detailed view for events generated by the COMPACT monitoring tools (in the BIT SENTINEL scenario). All views can be personalized by the LPA security administrators and by COMPACT monitoring tools providers. Two profiles will be available in the SOC Dashboard: the first one is the administrative profile that can be used to modify the views provided by the dashboard and to add new ones; the second one is the viewer profile that allows only the visualization of the dashboard views.

The SOC light version is ready to be installed on the LPA infrastructure. The installation will be performed during the first weeks of November 2018, in agreement with LPA availability. The trials timing will be compliant with the one defined in deliverable D5.1.

The SOC dashboard will be accessible using a local LPA address for the LPA employees and using a VPN address for the COMPACT partners. The list of addresses will be made available after the installation on LPA premises.
3.1.7. SENTINEL

Sentinel is a webmalware detection tool which helps scan the different web pages of an LPA for malware. LPAs can configure the analysis periodicity giving a chron. In addition, LPAs can also allow certain users to the platform.

If malware is found in an analysis to a LPA website a message is send through the communication bus directly to the SOC, in order to have a centralized information hub. In addition, a civil servant with permissions to access Sentinel platform can visualize the results.
of all the analysis performed, as well as, gathering information about the malicious code found in any analysis.

As mentioned before, Sentinel needs access to the Communication Bus built with Apache Kafka. For that reason, LPA will allocate Sentinel application on-premise and the will need to grant access to the communication bus, via VPN or LAN.

3.1.8. CyberConnector

CyberConnector (CC) is a collaborative environment where communities can share and improve knowledge in the cyber-security domain.

The environment built on CC and customised for COMPACT is the Information Hub: it provides a set of information sharing services that help users to share and build knowledge and implies the possibility for LPAs to find quickly in the CyberConnector information they might need in relation to existing best practices, guidelines and experiences produced by the other LPAs part of the COMPACT community.

The Information Hub has been developed to be used mainly by civil servants of the LPA but also by the rest of the stakeholders part of the COMPACT ecosystem: solution providers, researchers, central public administration and policy makers, legal experts and DPOs. Willing to collaborate in such European wide context, users participating in the Information Hub are expected to have sufficient English language knowledge: for this reason, the tool has no need to be translated. Still, envisioning also the participation of civil servants who may not have enough English knowledge, a multi-language access has been included to provide in local language (Italian, Portuguese, Spanish and German) at least a limited set of material. In this way, information about the project, contacts and the value of the services offered will be easy to understand for all the users, regardless the language they speak.

*Figure 8 - COMPACT Information Hub multi-language easy access*
Testing and adopting CC does not need any preliminary training, configuration nor installation: CyberConnector is a SaaS, available to all LPAs in the consortium and is not customized for single LPA. It is hosted by ENG’s servers and for the field trials, it will be available through the following link:

https://cyberconnector.eu/group/compact-information-hub/welcome

The tool will be opened to COMPACT partners in November 2018 for initial validation and will be available at the end of November 2018 for the start of the first trial phase.
A second version of the tool revised and tuned by feedback collected at the end of the first phase will be released at the end of April 2019.

3.1.9. Communication bus

The Communication bus will be installed on the same machine hosting the SOC, and will be compliant with the description provided in chapter 2.1.

3.1.10. Dashboard

As mentioned in chapter 2.2, COMPACT Dashboard gathers data from the COMPACT Communication Bus (refer to chapter 2.1). For that reason, COMPACT Dashboard needs to have access to the communication bus directly by LAN or by VPN. The COMPACT Dashboard will be installed on-premise in every LPA.
3.2. BOL – Municipality of Bologna

3.2.1. RATING

See chapter 3.1.1

3.2.2. TO4SEE

See description on chapter 3.1.2

For the field trials in the Municipality of Bologna (BOL), TO4SEE’s content has been translated into Italian and some of them localized to Italian context (see Figure 9 and Figure 10 for examples).

---

![Bolonia banner](image)

**Figure 9 - Example of TO4SEE's content localization for Italy**
3.2.3. Openness.edu

The description in section 3.1.4 is valid also for the field trial in the Municipality of Bologna. The only difference is the language used by BOL’s employees is Italian.

3.2.4. CSMG

Interactive workshop (a combination of computer-based and instructed learning) focuses line management on the importance of cybersecurity in their jobs and develops the competences essential to maintaining secure working practices in their divisions.

CSMG provides managers with an understanding of cybersecurity measures, and a straightforward set of actions for their adoption in the workplace, develops cybersafe decision-making, positioning cybersecurity issues as an integral part of business processes.

CSMG scenario renovation is being performed under COMPACT project, viewing the threats that people can face at their workplaces.

The game will be localized into Italian languages. There are following scenario components to be localised:

- Scenario components
  - Game Board
  - Game Rules PPT
  - Game Slides
  - Interface Constants
  - Certificates default texts
The localization is to be performed by partner LPA after they are provided with all the source files (Adobe Illustrator files for graphics, XLS files for Constants and PPT file for Game Rules).

CSMG is a SaaS application, that can be provided via Kaspersky Lab server.

To run CSMG the specialised training for trainers is required (2 days of onsite session).

**Timeframe:**

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alfa-version of CSMG LPA Scenario</td>
<td>Nov 2018</td>
</tr>
<tr>
<td>TTT for trainers from partner LPAs</td>
<td>20–21 Nov 2018, Milano</td>
</tr>
<tr>
<td>Trials for LPAs</td>
<td>Dec 2018 – Jan 2019</td>
</tr>
<tr>
<td>Feedback processing and implementation of changes</td>
<td>Jan–March 2019</td>
</tr>
<tr>
<td>Integration (data level) with Compact platform</td>
<td>Feb–Apr 2019</td>
</tr>
</tbody>
</table>

CSMG is a session-based on-site or online game that is not available out of the session time. More information: [https://www.kaspersky.com/enterprise-security/security-awareness](https://www.kaspersky.com/enterprise-security/security-awareness)

**3.2.5. CyberConnector**

The description provided in chapter 3.1.8 is valid also for this field trial.

**3.2.6. Communication Bus**

The Communication Bus for this field trial will be compliant with the description provided in chapter 2.1 and will be installed on ENG’s servers, on the same machine where RATING will be installed: an agreement have been signed between BOL and ENG to legally bind the arrangement between the two partners.

**3.2.7. Dashboard**

The description provided in chapter 3.1.10 will also apply to the Municipality of Bologna, but the Dashboard will be hosted into ENG’s servers.
3.3. **CDA – Municipality of Afragola**

3.3.1. **RATING**

See chapter 3.1.1

3.3.2. **TO4SEE**

See description on chapter 3.1.2

As for the Municipality of Afragola the content of TO4SEE is the same as the Municipality of Bologna: content is translated and localized for Italy.

3.3.3. **KIPS**

Custom-built software simulates the impact cyber-attacks and associated management decisions can have on business performance and revenue. Gameplay develops an understanding of cybersecurity measures. KIPS establishes a better security understanding among senior managers and decision makers, increases awareness of the risks and security problems of running modern computerized systems.

Specialized KIPS scenario is being developed for LPAs under COMPACT project, viewing the threats especially important for understanding by LPA management.

The scenario will be localized into Italian.

There are following scenario components to be localised:

- Scenario components
  - Game Board
  - Action Cards
  - Messages
  - Game Rules PPT
  - Scenario constants
  - Interface Constants
  - Certificates default texts
  - Feedback Form

The localization is to be performed by partner LPA after they are provided with all the source files (Adobe Illustrator files for graphics, PHP files for messages, XLS files for Constants and PPT file for Game Rules).

KIPS is a SaaS application, that can be provided via Kaspersky Lab server.

To run KIPS the specialised training for trainers is required (2 remote sessions on Webex, 3 hours each).
## Timeframe:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alfa-version of KIPS LPA Scenario</td>
<td>Nov 2018</td>
</tr>
<tr>
<td>TTT for trainers from partner LPAs</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>Trials for LPAs</td>
<td>Dec 2018 – Jan 2019</td>
</tr>
<tr>
<td>Feedback processing and implementation of changes</td>
<td>Jan-March 2019</td>
</tr>
<tr>
<td>Integration (data level) with Compact platform</td>
<td>Feb-Apr 2019</td>
</tr>
</tbody>
</table>

**Link:** KIPS is a session-based on-site or online game that is not available out of the session time. More information: [https://www.kaspersky.com/enterprise-security/security-awareness](https://www.kaspersky.com/enterprise-security/security-awareness)

### 3.3.4. SOLE

Silensec Online Learning Environment is a cloud based training platform. As such no local setup is required and users can access the training material directly. Access to the platform is done through user registration. Each user can independently register onto the platform and have access to the freely available training courses. With regards to COMPACT, the following two training courses have been developed and made available to project partners:

- Complying with GDPR Requirements
- Using the MISP Platform

While registration is user-driven, the enrollment to specific courses is done by a SOLE administrator. Specifically, the SOLE administrator will enroll all COMPACT trial users onto the above courses. Because SOLE provides access to virtual environments, users also have to download and configure a VPN certificate. This is a one-activity required specifically for accessing the training course on the MISP platform. The following figures show sample screenshots from the MISP-related training available on SOLE for the COMPACT users.

*Figure 11 - MISP-related training available on SOLE for the COMPACT users*
Two instructional videos have also been created to help users learn how to download and install the required VPN Certificates as shown below. Both videos have been published on YouTube and will be shared with registered users before the trials.

![VPN instructional videos](image)

**Figure 12 - VPN instructional videos**

For the CDA – Municipality of Afragola, the Silensec Online Learning Environment (SOLE) will make available the following:

a) Online hands-on Training on MISP  
b) Online training on GDPR Compliance  
c) Security Awareness Baseline Assessment

The following table summarizes the timeline of delivery of the SOLE-related activities for the trials:

<table>
<thead>
<tr>
<th>Timeframe</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>All training and assessment available in the original English Language</td>
<td>16&lt;sup&gt;th&lt;/sup&gt; Nov 2018</td>
</tr>
<tr>
<td>Localization of the Training courses and assessment in the Italian language</td>
<td>30&lt;sup&gt;th&lt;/sup&gt; Nov 2018</td>
</tr>
<tr>
<td>Trials for LPAs</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>Feedback processing and implementation of changes</td>
<td>Jan-March 2019</td>
</tr>
<tr>
<td>Integration (data level) with Compact platform</td>
<td>Feb-Apr 2019</td>
</tr>
</tbody>
</table>

All content will be available to registered and enrolled users via [https://sole.silensec.com](https://sole.silensec.com)
3.3.5. SOC

Inside the CDA LPA, the full SOC components will be installed. As agreed with CDA a VMware virtual machine will be configured and installed on the CDA private cluster and connected to the local LPA network and to the COMPACT VPN. The virtual machine will contains all tools needed by the SOC (Apache Flink, Logstash, ElasticSearch, Grafana), the COMPACT communication bus, and the COMPACT dashboard.

About the SOC data sources, during the CDA scenario the following sources will be monitored and correlated:

1. USB usage
2. Windows defender (antivirus)
3. OpenIntel

All the monitored LPA machines will be configured in order to enable specific Windows events logging and to forward these logs to the SOC using a specific SOC adapter that must be installed in each machine. An example of the machine configuration is reported below. It describes the steps needed to gather the information of the USB usage on a Windows machine using the native logging functionalities.

1. Open “Local security criteria”
2. Enable “Removable archive control” under “advanced configuration->Objects access”
3. Close “Local security criteria”
4. Open a shell code and run following command: “gpupdate /force”
5. Open “the Windows event visualizer”
6. Enable the registry “Operative” under “registries applications and services ->Microsoft->windows->driverFramework-UserMode->Operative”

In the following code (Code 1) is reported the configuration of the SOC Adapter that will be installed in each monitored machine.

```
winlogbeat.event_logs:
# - name: Application
#   ignore_older: 72h
- name: Microsoft-Windows-DriverFrameworks-UserMode/Operational
  ignore_older: 1h
- name: security
  ignore_older: 1h
- name: Microsoft-Windows-Windows Defender/Operational

output.logstash:
# The Logstash hosts
hosts: ["remote ip:5044"]
```

*Code 1 - SOC adapter configuration*
In Code 2 is reported the configuration of the SOC parser needed in order to receive data from the SOC probe, to parse in a JSON format and to forward it to the COMPACT Communication bus. This configuration files can be changed by the LAP security administrator in order to add any other sources that his/her considers of interest for the monitoring/correlation purposes.

The SOC (virtual machine) is ready to be installed on the LPA infrastructure. The installation will be performed during the first weeks of November 2018, in agreement with LPA availability. The trials timing will be compliant with the one defined in deliverable D5.1.

The SOC dashboard (see Figure 13) will be accessible using a local LPA address for the LPA employees (accessible for remote view using LPA procedures) and using a VPN address for the COMPACT partners. The list of addresses will be made available after the installation on LPA premises.

Two profiles will be available in the SOC Dashboard: the first one is the administrative profile that can be used to modify the views provided by the dashboard and to add new ones; the second one is the viewer profile that allows only the visualization of the dashboard views.
input { beats { port => 5044 } }
filter {
  json {
    source => "message"
    target => "__json"
    skip_on_invalid_json => true
    #remove_field => ["timestamp"]
  }
  if [log_name] == "Microsoft-Windows-DriverFrameworks-UserMode/Operational"{
    prune {
      interpolate => true
      whitelist_names => ["log_name", "level", "computer_name", "user_data", "xml_name", "@timestamp"]
    }
    mutate {
      add_field => {
        "lpaName" => "CDA-mun"
        "usb_code" => "%{[user_data]xml_name}"
        "InstanceId" => "%{[user_data]InstanceId}"
      }
      remove_field => [user_data]
    }
  } else if [log_name] == "Microsoft-Windows-Windows Defender/Operational"{
    prune {
      interpolate => true
      whitelist_names => ["log_name", "event_id", "message", "level", "computer_name", "@timestamp"]
    }
    mutate {
      add_field => {
        "lpaName" => "CDA-mun"
      }
    }
  } else {
    mutate {
      add_field => {
        "lpaName" => "CDA-mun"
      }
    }
  }
}
output {
  stdout {
    id => "CDA-Mun"
    codec => rubydebug
  }
  if [log_name] == "Microsoft-Windows-DriverFrameworks-UserMode/Operational"{
    kafka {
      bootstrap_servers => "Communication bus ip:9092"
      codec => json
      topic_id => "usb_monitor"
    }
  } else if [log_name] == "Microsoft-Windows-Windows Defender/Operational"{
    kafka {
      bootstrap_servers => "Communication bus ip:9092"
      codec => json
      topic_id => "WinDefender"
    }
  }
}

Code 2: SOC parser configuration
3.3.6. Openintel

The OpenIntel Platform runs on Silensec cloud infrastructure and will be made available to COMPACT users through a SaaS model. Also in this case no local configuration or set up is required. All COMPACT trial users will be registered for access onto the platform and be able to search for IoC related to their organization.

A user guide will also be made available to every registered users to help them use the platform.

The delivery of the trials will involve the following activities:

a) User Enrolment – In this activity, users are enrolled onto Openintel Training course

b) Induction – in this section Silensec will introduce participants to the SOLE Learning environment where OpenIntel training is hosted.

c) Self-paced learning – Users work through the training courses and activities developed for the,

The following table summarizes the timeline of the activities.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Enrolment</td>
<td>16&lt;sup&gt;th&lt;/sup&gt; Nov 2018</td>
</tr>
<tr>
<td>Induction</td>
<td>30&lt;sup&gt;th&lt;/sup&gt; Nov 2018</td>
</tr>
<tr>
<td>Self-Paced Learning</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>Feedback processing and implementation of changes</td>
<td>Jan-March 2019</td>
</tr>
<tr>
<td>Integration (data level) with Compact platform</td>
<td>Feb-Apr 2019</td>
</tr>
</tbody>
</table>
3.3.7. CyberConnector

The description provided in chapter 3.1.8 is valid also for this field trial.

3.3.8. Communication bus

The Communication bus will be installed on the same machine hosting the SOC, and will be compliant with the description provided in chapter 2.1.

3.3.9. Dashboard

The description provided in chapter 3.1.10 will also apply to the Municipality of Afragola.
3.4. **CMA – Municipality of Amadora**

3.4.1. **RATING**

See chapter 3.1.1

3.4.2. **TO4SEE**

See description on chapter 3.1.2

For the field trials in the Municipality of Amadora (CMA), TO4SEE’s content has been translated into Portuguese and some of them localized to Portuguese context.

3.4.3. **SOC**

For the CMA LPA, the SOC component will be used only as presentation layer of the other security monitoring tools involved in the CMA scenario. The description provided for the BIT LPA (chapter 3.1.6) is valid also for this scenario.

3.4.4. **BP-IDS**

BP-IDS is a process monitoring solution that aims at the detection of incidents on technology enabled infrastructures. It operates by collecting traces from multiple sensors scattered on the monitored infrastructure that indicate execution of activities in business processes and in real time matches the activities detected in the executed business process with the specified business process and specified business rules. Whenever those executed process deviate from the specification, the activity is marked as a possible incident and the infrastructure administrator is notified in real-time by BP-IDS with the causes of that anomaly (traces, affected processes, etc.). Thus, offering broad protection against: cybersecurity incidents (such as, intrusions or forgery of equipment behaviour); and operational security incidents (like, equipment and network failure, human error, or natural disasters).

On the scope of the COMPACT trials’ setup, INOV has installed, locally on the CMA premises, the new version of the BP-IDS tool (featured on COMPACT’s intermedium release). The installation adapted BP-IDS the IT infrastructure currently employed on the CMA municipality, which was described on the trial scenario specifications. The version deployed monitors the interaction between the municipality’s computers and municipal database (where the business activities are registered) to identify incidents related with the municipality’s processes: emission of certificates; and assiduity management.

---

1The detailed scenario description can be found on the deliverable: D5.1 Validation and Demonstration scenarios
To achieve this, BP-IDS was deployed with a special sensor capable of identifying business activities in operations made from computers to the database. All operations are identified by custom tracers installed on CMA computers, that continuously monitor the device and autonomously report database operations to the sensor.

During the first trial, BP-IDS will be configured to identify incidents related with GDPR infringement, specifically the right to be forgotten, based on the activities from those business processes. While on the second trial, based on the feedback from the first trial BP-IDS will be configured to also identify GDPR incidents related with _Purpose limitation_ monitoring (i.e., checking the data processor’s legal ground for processing data subject’s data).

The remainder of this section describes in detail the deployment made on Amadora municipality and the configuration necessary to monitor the selected business processes. Section 0 describes the BP-IDS components and the overall solution architecture; Section 3.4.4.2 explains step-by-step how the deployment was carried out; Section 3.4.4.3 explains how the tool will be configured with the necessary specification to monitor those business processes; Section 3.4.4.4 provides an action plan of the activities required for setting up the tool for the first and second COMPACT trial.

### 3.4.4.1. Architecture and description

*Figure 14 - Diagram representing the BP-IDS installation made on the IT infrastructure of the municipality of Amadora. Connection between systems coloured in black are interactions that currently occur in the IT infrastructure. While the blue connections, are the additional connections required for BP-IDS to monitor database activity.*
As can be seen illustrated in Figure 14, the BP-IDS is a distributed application scattered across the monitored infrastructure, composed of four components:

- Several tracers also called ‘Database Trace Gatherer components’, that continuously monitor the operation made from a computer (where they are installed) to the CMA database.
- One sensor that identifies evidences of business activities based on the database interactions intercepted by the tracer.
- One monitoring core that provides incident detection by comparing evidences captured by the sensor with business process specifications.
- One management component containing two types utilities:
  - Administration Interface utility, that allows LPA employees to setup BP-IDS with the necessary specifications for incident detection.
  - Monitoring Interface utility, that allows LPA employees to follow the monitoring process employed by the BP-IDS tool and conduct forensic investigations to assess the cause and impact the incident had on the organizations devices and business goals.

3.4.4.2. Installation Process

To facilitate the installation of BP-IDS in the CMA infrastructure, INOV provided an installation package containing all the components in a plug-n-play fashion. The sensor, monitoring core and management component were distributed as virtual machines pre-configured with all the necessary information to inspect the business processes selected for the trials and were hosted on an LPA server. While the tracer component featured on the package install was provided as a Dynamic Link Library (DLL) and installed on all the computers that interacted with the database during the COMPACT trials.

BP-IDS Virtual Machines Installation

The virtual machines included on the installation packaged had the following characteristics:

- Monitoring core:
  - Processor: Intel Xeon E312xx (Sandy Bridge) 2497.104MHz cache 4096 KB
  - RAM: 4GB
  - Storage: 60GB
  - Network interface: 1
  - OS: Linux

\[2\] Short description on the architecture of the BP-IDS component provided in the COMPACT intermediate release. Please refer to the deliverable “D4.3 COMPACT Threat intelligence and monitoring Adaptation (v1)” for a more detailed description.
• Sensor:
  o Processor: Intel Xeon E312xx (Sandy Bridge) 2497.104MHz cache 4096 KB
  o RAM: 4GB
  o Storage: 21.5GB
  o Network interface: 1
  o OS: Linux

• Management component:
  o Processor: Intel Core Processor (Haswell) 2497.104 MHz cache 4096 KB
  o RAM: 4GB
  o Storage: 8GB
  o Network interface: 1
  o OS: Linux

BP-IDS DLL Installation

![ODBC Data Source Administrator](image)

*Figure 15 - Configuration required for tracer DLL activation using the ODBC Data Source Administrator*

BP-IDS tracer DLL was included on all the LPA’s computers that interacted with the database\(^3\) and enabled using the “ODBC Data Source Administrator” application already included on most Windows operating systems and on all the computers selected for the trials. As seen in

\(^3\) Although this installation process is only compatible with Windows computers, CMA only uses this operating system.
Figure 15, to enable the tracer component on this Microsoft application the following information of the “Tracing” separator should be specified as follows:

- “Custom Trace DLL”, should contain the full path where the DLL is stored.
- “Log File Path”, should contain the location where the sensor is expected to read the traces produced by the tracer.

After filling the information, the tracer can be activated by pressing the “Start Tracing Now” button to start intercepting the database interactions established by the computer and send them in real-time to the BP-IDS sensor to start the business process monitoring.

### 3.4.4.3. Configuring BP-IDS with Business Processes Specification

The BP-IDS version included on the installation package was configured to monitor the business process of: emission of certificates; and assiduity management. To do so, INOV configured BP-IDS using the Administration Interface utility with the necessary specification required for monitoring those processes. The specification includes information regarding the CMA network topology and business process information.

![Network Diagram](image)

*Figure 16 - CMA network topology, describing all the information required to establish communication between all BP-IDS components and to determine where to collect the traces. The information provided includes, the IP address and location in the network of all BP-IDS components.*

The network topology specification included in the BP-IDS installation was built in the Administration Interface and included: the graphical representation (depicted in the Figure 16) describing the devices and connections monitored during the first trial; and for each device included information regarding its IP address and the location of the logs produced by the tracers. Specifically, BP-IDS was configured with the following network information:

- Tracers: RDS Computer 1-3, connected to the RDS network.
• BP-IDS components:
  o Sensor Plugin, connected to the RDS network
  o Monitoring core, connected only to the other BP-IDS components.
  o Management utilities, connected to the RDS Server.

Table 3 - Business process information, describing for each monitored process all the information required to identify the activities and resources linked to the monitored process and to perform incident detection. The figure on the left shows the information related with the process ‘Emission of certification’, while the figure on the right is related with process ‘Assiduity Management’.

The business process specification included in the BP-IDS installation includes for each monitored process: identification of the resources referenced by the process; and a graphical representation of the process in a BPMN diagram (as represented in Table 3 - Business process information, describing for each monitored process all the information required to identify the activities and resources linked to the monitored process and to perform incident detection. The figure on the left shows the information related with the process ‘Emission of certification’, while the figure on the right is related with process ‘Assiduity Management’.

) describing the activities involved in the process and establishing the necessary conditions to validate the process. Namely the diagram establishes the order that the activities should happen in order to consider the activities valid (e.g., in the emission of certificates process, the activity ‘Sign Certificate’ can only be executed if the ‘Create Certificate’ has already happened). Specifically, BP-IDS was configured with the following business process information:

- Process: Emission of Certificates
  - Resources involved:
    ▪ Certificate – official classification issued by CMA to a specific person
    ▪ Employee – entity that creates and signs the certificate
    ▪ Person – entity that referenced in the certificate
  - Key attribute:
    ▪ ‘certificateID’: Each process refers to the emission of a specific certificate and is identified by the identification number of that certificate.

• Activities:
  ▪ ‘Create Certificate’
    • Conditions: First activity of the process, must only happen if no other certificates have been created with the same ID.
  ▪ ‘Sign Certificate’
    • Conditions: Second activity can only happen after the certificate has been created by issuing the ‘Create Certificate’.

• Process: Assiduity Management
  o Resources (informational entity Types) involved: Employee, Person
  o Key attribute:
    ▪ ‘month’, ‘year’, ‘VAT Number’: Each process refers to the payment of the monthly salary associated to a person that has worked in CMA on a specific month and is identified by the date (month and year) and VAT number of the person receiving the salary.

  o Activities:
    ▪ ‘Check month assiduity’
      • Conditions: First activity of the process, repeated until the employee receiving the salary completes his assiduity (gateway ‘Assiduity Complete?’).
    ▪ ‘Emit salary’
      • Conditions: Second activity of the process, can only happen after assiduity has been validated by the activity ‘Check month assiduity’.

3.4.4.4. Action Plan

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Name</th>
<th>Duration</th>
<th>Start</th>
<th>Finish</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Milestone</td>
<td>BP-IDS Intermediate</td>
<td>0 days</td>
<td>Mon 10/15/18</td>
<td>Mon 10/15/18</td>
</tr>
<tr>
<td>2</td>
<td>Activity</td>
<td>Configure BP-IDS</td>
<td>1.7 mos</td>
<td>Tue 10/16/18</td>
<td>Fri 11/30/18</td>
</tr>
<tr>
<td>3</td>
<td>Activity</td>
<td>First Compact Trials</td>
<td>21 days</td>
<td>Mon 12/3/18</td>
<td>Mon 12/31/18</td>
</tr>
<tr>
<td>4</td>
<td>Milestone</td>
<td>Final Release</td>
<td>0 days</td>
<td>Fri 3/29/19</td>
<td>Fri 3/29/19</td>
</tr>
<tr>
<td>5</td>
<td>Activity</td>
<td>Configure BP-IDS</td>
<td>1.05 mos</td>
<td>Tue 4/2/19</td>
<td>Tue 4/30/19</td>
</tr>
<tr>
<td>6</td>
<td>Activity</td>
<td>Second Compact Trials</td>
<td>21 days</td>
<td>Wed 5/1/19</td>
<td>Wed 5/29/19</td>
</tr>
</tbody>
</table>

Figure 17 - GANTT diagram that schedules all the action plan tasks proposed in this document. The tasks are distributed across the vertical axis, while the horizontal axis shows the evolution of time in months from the first release of the COMPACT platform to the last COMPACT trial.
To ensure BP-IDS is configured and ready for testing in the two upcoming COMPACT trials, INOV proposes the action plan depicted in Figure 17, composed of 3 activities and 2 milestones. The plan should be executed as follows:

**Milestone 1 – Final Release (M24)** – In this milestone INOV will deploy the complete version of the BP-IDS tool.

**Activity 2 – Configure BP-IDS (M19-M20)** – INOV will configure BP-IDS to monitor the business processes selected for the first COMPACT trial, based on the information gathered from CMA about their IT infrastructure. Although most work has already been performed as reported before in this section, there is still some configuration to be performed. Namely, the construction of identification patterns used by the sensor to identify the activities of the business processes selected for the trials, and the creation and finetuning of the monitoring components to identify GDPR incidents related with the access of personal data when the processes are performed.

**Activity 3 – First COMPACT trial (M21-M22)** – CMA will test BP-IDS by performing processes of emission of certificates and assiduity management. INOV will gather feedback from the users that tested the tool and obtain the results of profiling the tool usage during the testing, and evaluate how BP-IDS performed in the trials. The information of the testing and the feedback gathered from Amadora trials will be presented in the upcoming deliverable ‘D5.3 Pilot execution v1’ (M22).

**Milestone 4 – Final Release (M24)** – In this milestone INOV will deploy the complete version of the BP-IDS tool.

**Activity 5 – Configure BP-IDS (M25)** – In this task INOV will configure BP-IDS to monitor the business processes selected for the second COMPACT trial. Although some configuration may be reused from the first compact trial, it is expected that the developments made to the tool between the first and second trials require additional configurations to prepare for the second trial.

**Activity 6 – Second Trials (M26-M27)** – CMA will test BP-IDS by performing processes of emission of certificates and assiduity management. INOV will gather feedback from the users that tested the tool and obtain the results of profiling the tool usage during the testing and evaluate how BP-IDS performed in the trials. The information of the testing and the feedback gathered from Amadora trials will be presented in the deliverable ‘D5.3 Pilot execution v2’.
3.4.5. **MISP**

The Malware Information Sharing Platform will be made available on the public domain misp.compact.com. The following screenshots show the sample deployment that will be visible to the COMPACT users.

As it can be seen from the above figure, through MISP, LPAs will be able to share information within their organization or within the LPA community. A specific MISP instance will be instantiated and maintained for each LPA within the COMPACT trials.

MISP installations will be provided as a SaaS by COMPACT and all COMPACT trial users will be given access. Therefore no local set up will be required. The only pre-requisite for accessing MISP will be the enrolment and attendance of the MISP-related training available on Silensec Online Learning Environment (SOLE) also part of the COMPACT trials.

The delivery of the trial will involve the following activities:

a) **User Enrolment** – In this activity, users are enrolled onto MISP and Openintel Training courses as well as onto the MISP platform.

b) **Induction** – in this section Silensec will introduce participants to the SOLE Learning environment where MISP and OpenIntel training is hosted. The users are also shown how to download and installed the required user VPN certificate and how to use the course.

c) **Self-paced learning** – Users work through the training courses and activities developed for the,

d) **MISP Practical Challenge** – Understanding the key concepts of MISP and being able to correctly use it requires some time. In this activity the participants are given a practical challenge to test their ability to use MISP for the purposes of sharing intelligence with other LPAs.
The following table summarizes the timeline of the activities.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Enrolment</td>
<td>16&lt;sup&gt;th&lt;/sup&gt; Nov 2018</td>
</tr>
<tr>
<td>Induction</td>
<td>30&lt;sup&gt;th&lt;/sup&gt; Nov 2018</td>
</tr>
<tr>
<td>Self-Paced Learning</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>MISP Practical Challenge</td>
<td>Jan 2019</td>
</tr>
<tr>
<td>Feedback processing and implementation of changes</td>
<td>Jan-March 2019</td>
</tr>
<tr>
<td>Integration (data level) with Compact platform</td>
<td>Feb-Apr 2019</td>
</tr>
</tbody>
</table>

3.4.6. Communication bus

The Communication bus will be installed on the same machine hosting the SOC, and will be compliant with the description provided in chapter 2.1.

3.4.7. Dashboard

The description provided in chapter 3.1.10 will also apply to the Municipality of Amadora.
3.5. **DSS – Municipality of San Sebastian**

3.5.1. **RATING**

See chapter 3.1.1

3.5.2. **TO4SEE**

See description on chapter 3.1.2

For the field trials in the Municipality of San Sebastian (DSS), TO4SEE’s content has been translated into Spanish and Basque and some of them localized to Spanish context (see Figure 19-20-21 for examples).

![Figure 19 - Example of TO4SEE’s content localization for Portugal](image-url)
Figure 20 - Second example of TO4SEE’s content localization for Portugal

Figure 21 - Third example of TO4SEE’s content localization for Portugal

3.5.3. HFP

The provision of HFP will be similar to the one provided for BIT. The HFP for DSS will be provided in both Spanish and Basque Version.
The Human Factor Profile is a survey instrument which can be used to investigate human predictors of security-related behaviour. In particular, HFP depicts six human factors that have been proven to influence security-related behaviour. Results should guide the management of an organisation to choose suitable awareness methods. In addition, it provides the management with data that describe work-related, organizational, and other individual variables that are relevant in this context.

- **Configuration**: Configuration: please specify if the tool will be customized for that LPA and how; The tool will not be customized for the specific LPA, as the human factors that are analysed are generalizable across organizations.

- **Installation**: There is no installation or training needed. To guide users, we provide an instruction about how to proceed with the HFP.

- **The tool will be ready in November, whereas the process for analysis will be done manually. Here is the link to the HFP tool (here is the English version of the survey: https://surveys.tech-experience.at/index.php/731494?lang=en). A detailed description can be found in D4.2.

Instruction for using HFP presented to the LPAs to guide them in using HFP:

<table>
<thead>
<tr>
<th>General Information: The Human Factor Profiling method is a Survey Instrument that should help you to understand why people within your organisation act security-aware. This information should guide you in choosing the most suitable awareness method for your employees. The link is meant to be spread to the employees in your organisation. Please be aware that due to anonymity reasons we will only analyze the data and provide you with results when more than three employees filled out the survey.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedure: Before using this survey please be aware of informing all relevant stakeholders within your organization including the workers’ council or the data protection officer. This can increase the acceptance of this survey significantly. We also recommend informing employees about the results of the survey in a workshop setting.</td>
</tr>
<tr>
<td>Return Rates: The higher the return rates the higher is the validity of the results for your specific organisation. We recommend sending two reminders; one after one week and one two days before the survey will be closed.</td>
</tr>
<tr>
<td>For the creation of the survey link and for our analyses we need some information from you: Name of your organisation in this field (also a fictional name is possible): __________ Number of employees that will get the link to the survey: ______</td>
</tr>
<tr>
<td>Here is the Human Factor Profiling survey link: ______________ Please spread this link in your organisation for example via e-mail or intranet. Thereby, you can use the following text and adapt it according to your personal preferences:</td>
</tr>
</tbody>
</table>

“Maintaining security in an organisation is increasingly important. We at <organisation name> are interested in investigating how to provide you with suitable training to increase security-related behaviour and thus make our organisation resilient against a potential cyber-attack. This survey should help us to understand why people within our organisation act security-aware and how to support them in acting more security-aware. The
information collected within the survey guides us to choose the most suitable awareness methods we can use in training. So, the more survey data we get the more tailored our training can be. 

Here is the link to the survey which will be sent to all employees: <insert survey link in here>. The survey is open for two weeks.

Please be aware that this data will be analysed in an aggregated way with at least three data sets. So, there is no possibility to draw conclusions to the individual employee. If you have any questions please contact me.”

3.5.4. KIPS

Custom-built software simulates the impact cyber-attacks and associated management decisions can have on business performance and revenue. Gameplay develops an understanding of cybersecurity measures. KIPS establishes a better security understanding among senior managers and decision makers, increases awareness of the risks and security problems of running modern computerized systems.

Specialized KIPS scenario is being developed for LPAs under COMPACT project, viewing the threats especially important for understanding by LPA management

The scenario will be localized into Spanish and Basque. There are following scenario components to be localised:

- Scenario components
  - Game Board
  - Action Cards
  - Messages
  - Game Rules PPT
  - Scenario constants
  - Interface Constants (to Bask only)
  - Certificates default texts (to Bask only)
  - Feedback Form (to Bask only)

The localization is to be performed by partner LPA after they are provided with all the source files (e.g. Adobe Illustrator files for graphics, PHP files for messages, XLS files for Constants and PPT file for Game Rules)

KIPS is a SaaS application, that can be provided via Kaspersky Lab server. To run KIPS the specialised training for trainers is required (2 remote sessions on Webex, 3 hours each).

Timeframe:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alfa-version of KIPS LPA Scenario</td>
<td>Nov 2018</td>
</tr>
<tr>
<td>TTT for trainers from partner LPAs</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>Trials for LPAs</td>
<td>Dec 2018 – Jan 2019</td>
</tr>
</tbody>
</table>
Feedback processing and implementation of changes | Jan-March 2019
---|---
Integration (data level) with Compact platform | Feb-Apr 2019

Link: KIPS is a session-based on-site or online game that is not available out of the session time. More information: [https://www.kaspersky.com/enterprise-security/security-awareness](https://www.kaspersky.com/enterprise-security/security-awareness)

### 3.5.5. SOLE

For the DSS – Municipality of San Sebastian, the Silensec Online Learning Environment (SOLE) will make available the following:

a) Online training on GDPR Compliance  
b) Security Awareness Baseline Assessment

The following table summarizes the timeline of delivery of the SOLE-related activities for the trials:

#### Timeframe:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>All training and assessment available in the original English Language</td>
<td>16th Nov 2018</td>
</tr>
<tr>
<td>Trials for LPAs</td>
<td>Dec 2018</td>
</tr>
<tr>
<td>Feedback processing and implementation of changes</td>
<td>Jan-March 2019</td>
</tr>
<tr>
<td>Integration (data level) with Compact platform</td>
<td>Feb-Apr 2019</td>
</tr>
</tbody>
</table>

All content will be available via [https://sole.silensec.com](https://sole.silensec.com)

The delivery of the trials will involve the following activities:

a) User Enrolment – In this activity, users are enrolled onto MISP and Openintel Training courses as well as onto the MISP platform;  
b) Induction – in this section Silensec will introduce participants to the SOLE Learning environment;  
c) Self-paced learning – Users work through the training courses and activities developed for the,

The following table summarizes the timeline of the activities.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Enrolment</td>
<td>16th Nov 2018</td>
</tr>
<tr>
<td>Induction</td>
<td>30th Nov 2018</td>
</tr>
<tr>
<td>Self-Paced Learning</td>
<td>Dec 2018</td>
</tr>
</tbody>
</table>
Feedback processing and implementation of changes | Jan-March 2019
Integration (data level) with Compact platform | Feb-Apr 2019

3.5.6. SOC

For the CMA LPA, the SOC component will be used only as presentation layer of the other security monitoring tools involved in the CMA scenario. The description provided for the BIT LPA (chapter 3.1.6) is valid also for this scenario.

3.5.7. SENTINEL

The description provided in chapter 3.1.7 will also apply to the Municipality of San Sebastian.

3.5.8. Communication bus

The Communication bus will be installed on the same machine hosting the SOC, and will be compliant with the description provided in chapter 2.1.

3.5.9. Dashboard

The description provided in chapter 3.1.10 will also apply to the Municipality of San Sebastian.
4. Checklist for research involving human participants

<table>
<thead>
<tr>
<th>Risk</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Potentially severe impact of research results on human rights of individuals or groups (e.g. privacy issues, discrimination, stigmatisation) | • Risk assessment (fill in the DPIA)  
• Indicate the methods used for correct interpretation of research results, to avoid/reduce the negative impact on human rights  
• Indicate the methods used regarding the dissemination and publication of results, to reduce the negative impact on human rights  
• State that no data other than the results of the project (software and documentation) will be exported to non-EU Member States |

Please justify your measure(s):  
We do not expect severe impact of research results on human rights, as we use appropriate methods for data handling. The data will be pseudonymised and kept confidential within the project team. The dissemination and publication of results will only be in aggregated form, thus assuring anonymity of participants. Only these aggregated results of the project will be exported to non-EU Member States through scientific publications.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential misuse or abuse of research</td>
<td>• Indicate the measures used to reduce/avoid the potential misuse or abuse of the research</td>
</tr>
</tbody>
</table>

Please justify your measure(s):  
The data will be stored in a protected folder by each LPA team and only used for research purposes related to the evaluation of the COMPACT online study.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-compliance with data protection legislation</td>
<td>• Risk assessment (fill in the DPIA)</td>
</tr>
</tbody>
</table>

Please justify your measure(s):  
Already covered in DPIA

<table>
<thead>
<tr>
<th>Risk</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-compliance with data protection legislation</td>
<td>• Risk assessment (fill in the DPIA)</td>
</tr>
</tbody>
</table>
Regarding human volunteers

Please justify your measure(s):

Due to the sole processing of data, that every LPA cannot relate to identified natural persons ("indirectly personal data"), a notification with the Italian Data Protection Authority is not necessary.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Disclosure of confidential documents |  - Indicate the methods used regarding the dissemination and publication of results, to avoid the disclosure of confidential information of partners  
  - State that partners complied with non-disclosure agreements and internal contracts in relation to research data |

Please justify your measure(s):

The disclosure of confidential information of partners (especially the participating end user organizations) is avoided by aggregating the research results over participants from all participating organizations. The goal of the research is to assess the awareness and knowledge about cyber security of LPAs in general, not to compare LPAs from different organizations. Every LPA will comply with non-disclosure agreements provided by end user organizations.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data loss during execution of tests</td>
<td>- Indicate the methods used regarding the protection of the stored data and transfer of data</td>
</tr>
</tbody>
</table>

Please justify your measure(s):

The data collected will be stored within an industry standard database system with anonymous IDs and without any personal data. The database will be secured using industry standard access procedures. The data stored will have no reference to the personal information of a test user. Moreover, data collected in the project will not be accessible from the internet, due to security issues. The database will be locked from employees not involved in the project. Data will be transferred to project partners only partly and in an anonymised way via a secure channel.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Loss of personal data |  - Indicate detailed measures on storage assessment, including access control  
  - Provide details on the access control, e.g. safety measures |

Please justify your measure(s):
All data will be stored in a secure way, taking into account up to date security measures following the rules of the protection of personal data: national and international legislations emphasize the right of an individual that this personal data has to be protected. Every LPA guarantees the protection of personal data. All personal data collected from volunteers shall be made irreversibly anonymous and destroyed at the end of the project.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage of vast quantities of data for long time periods</td>
<td>• Indicate the procedures and methods for erasure and anonymization of data</td>
</tr>
</tbody>
</table>

Please justify your measure(s):
To Pseudonymize the data, participants are assigned a participant code to differentiate between participants instead of a name or email address. As research methods require to involve the same participants multiple times in different studies, the mapping between participant codes and personal information (Name, email address) is stored separately in a protected folder, only accessible by the responsible experimenter and a proxy. Sensitive data will be stored until all project activities are finalized and then erased.